Public, Private, and Permissioned Blockchains Compared

By Shobhit Seth Updated November 02, 2024

Public vs. Private vs. Permissioned: An Overview

Public blockchains allow anyone access; private blockchains are available to selected or authorized users; permissioned blockchains have different levels of user permissions or roles.

Many cryptocurrencies are built on open-source, public blockchains. Others are permissioned in that they are available to anyone to use, but roles are assigned, and only specific users can make changes.

Private and permissioned blockchains are generally used by organizations or businesses with specific needs.

Key Takeaways

- In a public blockchain, anyone can join and participate in the network's core activities.
- A private blockchain allows only selected and verified participants; the operator has the right to override, edit, or delete entries on the blockchain.
- Permissioned blockchains allocate specific roles or permissions to various users on the network.

Public Blockchain

A public blockchain is one where anyone is free to join and participate in the core activities of the blockchain network. Anyone can read, write, or audit the ongoing activities on a public blockchain network, which helps achieve the self-governed, decentralized nature often touted when cryptocurrency blockchains are discussed.

Advantages

A public blockchain operates on an incentivizing scheme that encourages new participants to join. Public blockchains offer a particularly valuable solution from the point of view of a truly decentralized, democratized, and authority-free operation.

Public blockchains are used in cryptocurrencies and decentralized finance because they can serve as a backbone for nearly any decentralized solution. Additionally, the vast number of network participants that can join a secured public blockchain keeps it safe from data breaches, hacking attempts, or other cybersecurity issues. The more participants, the safer a public blockchain is.

Public blockchains can be secured with automatic validation methods and encryption that keep single entities from changing information in the chain (like cryptocurrency blockchains), or they can allow anyone to make changes.

Disadvantages

One concern for public blockchains is security. Some designers have solved it using a competitive and distributed validation/block proposing/reward system, while others have solved it using a collateralized system.

Other issues include a lack of complete privacy and anonymity. Public blockchains allow anyone to view transaction amounts and the addresses involved. If the address owners become known, the user loses their anonymity.

Public blockchains also attract participants who may not be honest in their intentions. Most public blockchains are designed for cryptocurrencies, which, by nature of their value, are a prime target for hackers and thieves.

Private Blockchain

Participants can join a private blockchain network only through an invitation where their identity or other required information is authentic and verified. The validation is done by the network operator(s) or by a clearly defined set protocol implemented by the network through smart contracts or other automated approval methods.

Thus, private blockchains control who is allowed to participate in the network. The owner or operator has the right to override, edit, or delete the necessary entries on the blockchain as required or as they see fit to make changes to the programming.

Advantages

A private blockchain is not decentralized. It is a distributed ledger that operates as a closed database secured with cryptographic concepts and the organization's security measures. Only those with permission can run a full node, make transactions, or validate/authenticate the blockchain changes.

By reducing the focus on protecting user identities and promoting transparency, private blockchains prioritize efficiency and immutability—the state of not being able to be changed.

These are important features in supply, logistics, payroll, finances, accounting, and many other enterprise and business areas.

Disadvantages

While purposefully designed for enterprise applications, private blockchains lack many of the valuable attributes of permissionless systems simply because they are not widely applicable. Instead, they are built to accomplish specific tasks and functions.

In this respect, private blockchains are susceptible to data breaches and other security threats. This is because there are generally limited validators used to reach a consensus about transactions and data (if a consensus mechanism is needed). In a private blockchain, there may not be a need for consensus, only the immutability of entered data.

Permissioned Blockchain

Permissioned blockchains generally have characteristics similar to public and private blockchains, with many options for customization.

Advantages

Permissioned blockchain advantages include allowing anyone to join the permissioned network after a suitable identity verification process. Some give special and designated permissions to perform only specific activities on a network. This allows participants to perform particular functions such as reading, accessing, or entering information on the blockchain.

Permissioned blockchains allow for many functions, but one most interesting to businesses is Blockchain-as-a-Service (BaaS)—a blockchain designed to be scalable for the needs of many companies or tasks that the providers rent out to other businesses.

Blockchain-as-a-Service reduces costs for many businesses that can benefit from using blockchain technology in their business processes.

For example, imagine a business wants to improve transparency and accuracy in its accounting processes and financial reporting. It could rent blockchain accounting services from a BaaS provider. The blockchain would provide an interface where entries are made by end users and then automates the rest of the accounting processes using encryption, verification, and consensus techniques.

In this way, there would be fewer errors and no way for someone to alter financial data after it is entered. As a result, financial reports to management and executives become more accurate, and the blockchain is accessible for viewing and generating real-time financial reports.

The business could also choose to have the blockchain and supporting systems automate its invoicing, payments, bookkeeping, and tax reporting.

Disadvantages

The disadvantages of permissioned blockchains mirror those of public and private blockchains, depending on how they are configured. One key disadvantage is that because permissioned blockchains require internet connections, they are vulnerable to hacking. By design, some might use immutability techniques such as cryptographic security measures and validation through consensus mechanisms.

While most blockchains are thought to be unhackable, without the proper precautions, they have weaknesses. Cryptocurrency theft occurs when supporting applications and programs on a blockchain network are hacked into and private keys are stolen. Permissioned blockchains also suffer this weakness because the networks and applications that connect to the blockchain services depend on security measures that can be bypassed.

What Are the 4 Types of Blockchains?

There are three general types of blockchains: public, private, and permissioned. There are also hybrids of these three: public permissioned and private permissioned.

What Is a Public But Permissioned Blockchain?

A public but permissioned blockchain could take a few forms, but it would generally be publicly

viewable, and anyone could be granted permission to participate or access it.

What Are Permissioned Blockchains?

A permissioned blockchain is a public or private blockchain where multiple users are given permissions, roles, and abilities.

The Bottom Line

Public blockchains allow anyone to participate. Permissioned blockchains create different roles and have known users. Private blockchains are used by entities that need a secure ledger, allowing access to only those who need it.